THE COMMITTEE ON ENERGY AND COMMERCE

INTERNAL MEMORANDUM

May 2, 2011

To: Members of the Subcommittee on Commerce, Manufacturing, and Trade

From: Majority Committee Staff

Re: Hearing on "The Threat of Data Theft to American Consumers"

I. Summary

On Wednesday, May 4, 2011, at 9:30 a.m., the Subcommittee on Commerce, Manufacturing and Trade will hold a hearing entitled, "The Threat of Data Theft to American Consumers" in 2322 Rayburn House Office Building. Witnesses are by invitation only.

The purpose of this hearing is to examine risks related to data breaches, the state of ongoing investigations, current industry data security practices, and available technology.

II. Witnesses

Two panels of witnesses will testify before the Subcommittee.

Panel I

David Vladeck, Director, Bureau of Consumer Protection, Federal Trade Commission

Pablo Martinez, Deputy Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service

Panel 2

Justin Brookman, Director, Consumer Privacy Project, Center for Democracy and Technology

Dr. Gene Spafford, Executive Director, Purdue University

Additional witnesses may be added but are unavailable as of the time of circulation of this memo.

III. Background

Since this issue of data breach became a common household term in 2005 when hackers gained access to 160,000 consumer records in the ChoicePoint data breach, American consumers have been inundated with reports of data breaches on a regular basis. According to the Privacy Rights Clearinghouse, over 2,500 data breaches implicating nearly 600 million records have been

made public since 2005.[1,2] In April 2011 alone, the Clearinghouse reports over 30 data breaches occurred at hospitals and medical provider offices; universities; insurance companies; airlines; technology companies; banks; and at the municipal, State, and Federal government levels. These breaches occurred via phishing, theft of computer or other devices, and hacking, impacting a minimum of 99 million records (a number of these breaches impacted an "unknown" number of records).

These records involve various pieces of information that can be used alone or in conjunction with other pieces of information to wreak havoc on a consumer's financial well-being by using existing lines of credit or establishing new lines of credit, to gain unlawful access to bank accounts, to acquire jobs or government benefits for which they are otherwise not eligible, seek medical care, or use another's identification in a law enforcement situation. Data breaches often involve unauthorized access to a person's name, birth date, Social Security number, driver's license number, credit account numbers, financial account numbers, usernames and passwords, or PIN numbers.

Whether the breach occurs inadvertently through the accidental release of information, in the offline world by loss of a laptop or stolen records, or online via hacking, the results can be disastrous for consumers. The FTC estimates nearly 9 million Americans fall victim to identity theft annually, costing both consumers and businesses tens of billions of dollars each year. While the Identity Theft Resource Center reports that both the cost to consumers has fallen as has the number of hours lost in resolving identity thefts, consumers still lose hundreds of dollars out of pocket and spend dozens of hours on cleanup efforts.[3]

IV. Data Security Legislation

While more than 40 States have individual data breach notification requirements, with the exception of notification requirements for breached health information, there is no Federal data breach notification law. As a result of the confusing and often overlapping or contrary patchwork of State notification laws, Rep. Stearns (the then-Chairman of the Subcommittee on Commerce, Trade, and Consumer Protection) introduced H.R. 4127, the Data Accountability and Trust Act (DATA) in the 109th Congress. The bill established (1) security requirements for entities holding personal information to protect against unauthorized access; (2) notification procedures to affected consumers upon a breach; and (3) special requirements for information brokers. It charged the FTC with enforcement. The Committee reported H.R. 4127 on a bipartisan basis but the bill did not proceed to the full House for a vote as a result of disagreements with other committees regarding jurisdiction that could not be resolved before the Congressional calendar expired.

---

[1] http://www.privacyrights.org/sites/default/files/static/Chronology-of-Data-Breaches_-_Privacy-Rights-Clearinghouse.pdf

[2] A record is distinct from an individual. An individual may have several records impacted by one or more breaches (e.g., one consumer may have multiple credit card accounts, each of which may be serviced by one service provider, and thus could receive multiple notices from the service provider in the event the service provider's database is breached).

[3] http://www.idtheftcenter.org/artman2/publish/m_press/Aftermath_2009.shtml

In the 110th Congress, then-Chairman Rush re-introduced H.R. 4127 as H.R. 958 but the legislation received no Committee action. In the 111th Congress, Rep. Rush again reintroduced DATA as H.R. 2221, as amended from earlier versions (see Section-by-Section Analysis below). H.R. 2221 processed through the Committee on a bipartisan basis and passed the House by voice vote on December 8, 2009. As amended, H.R. 2221:

- Required entities that hold personal information to establish and maintain appropriate security policies to prevent unauthorized acquisition of that data.
- Required companies to notify consumers in the event of a breach of personally identifiable information that results in a reasonable risk of identity theft or fraud.
- Imposed special requirements on information brokers, those that compile and sell consumer data to third parties, including assuring accuracy of their information, allowing consumer access to their records and the ability to correct inaccurate information.
- Superseded State data breach and notification laws but permitted enforcement by State Attorneys General with an aggregate cap on damages.
- Preempted similar State laws to create a uniform national standard for data security and breach notification.
- Mandated reasonable security practices for paper records containing personally identifiable information.
- Permitted an information broker to include intentionally false information in a database if used for fraud detection purposes and the information is identified as inaccurate.
- Allowed for a delay in breach notification for law enforcement or national security purposes.
- Added passport numbers and military ID numbers to the definition of personal information.

Chairman Bono Mack intends to introduce a data security bill based on H.R. 2221 after receiving comments through Subcommittee oversight and a relevant stakeholder process.

Please contact Brian McCullough, Gib Mullan, or Shannon Weinberg at ext. 5-2927 with any questions.